During the mid-late 20th century, after World War II, nuclear weapons: the most devastating weapon mankind every created have treated the world for decades. However, moving into the 21st century, nuclear weapons were no longer the only biggest threat around us. Cyber threat, hackers, or even cyber warfare across multiple countries had taken over the place and became the biggest issues to national security. Amy Zegart, stated in her TED Talks--Cyberwar, there are three classes of cyber threats or attack to the U.S today: massive theft of intellectual property from an American corporation which might degrade our economic competitiveness for even generations; massive attack to the national basic infrastructures which may cause mass destruction toward society; attacks may also disable national securities and put the country into physical unprotected. With the cyber threat grew at an unbelievable speed, she also explains the key reasons behind this new threat.

Every year the Director of National intelligence has to issues a public threat assessment which runs down a list of danger to the country. In 2007, the list contains nothing relative to cyber. Two years after, cyber was on the button of the list. However, Amy mentions "cyber threats have grown in a speed of cyber ". Cyber threats have raised up to the top of the list in only a few years just after Stuxnet first exposed to the public. Which reply to the point mention in our main source: being the most powerful country in the world, the U.S should take responsibility to nowadays high tension between nations and even private sectors on cyberspace since the U.S starts the lead.

Meanwhile, Amy mentioned that “We  are the most vulnerable nation in cyberspace." The U.S has most offensive cyber strength among any other nation, but we can't still defend ourselves well. Today, the nation is relying on the internet in a tremendous and wide-ranging way. While the internet giving us huge convenience and connecting us to all over the world, the nation is also the most connected country in the world. Which means everyone has a computer can hack into our services, into the state's network relatively simple. This wide connections give us strengths to our society but also increase our weakness of defending this national security and also civilization privacy.

      Different than the physical world, defending in cyberspace is much harder which Amy explain her key reasons.  First of all, Traditional national threats are usually solved by the military. The U.S has the world most powerful military to protect this nation which gives us a reality saver environment to live. However, in cyberspace, the government can't just go along, since 85% of the national critical infrastructures are run by private sectors. The government can't defend all these services that keep our society functioning.  Secondly, on the internet, save place never existed. Computer scientists make a defect in every 2500 lines of code on average. Since we are connecting to all over the world, there always someone keeps looking for the defect and get something out of it, it's unavoidable. Thirdly, victims have no idea they are victims or at least not immediately. Hacking might only take minutes, then a virus could hide inside a computer for months and stealing information without any sign. Last but not least, different than physical war, cyber attacks have not warning time before attacks and response time usually take months. War could happen in a flash and may cause physical damage without any prepare which could lead to demonstrating consequences. Therefore, cyber threats are various, hard to prevent, traceback and could have deadly consequences.

Targets for cybercriminals comes widely. Some major areas that suffering cyber attack the most such as education system, power system, financial economic system, and the government military system. In November 2014, served DDoS attack brought down Rutgers University website for days. In June 2016, hackers lock up University of Calgary's school system for the exchange of $20000 untraceable bitcoin. In 2015, Canadian federal government websites and intelligence service brought done by a denial-of-service cyber attack. While hackers also attack 46 major financial institutions in the state. In the same year, cyber shut down the Ukrainian power grid left 700,000 people without any electricity for hours. There are countless cyber attacks happened in the past decade, caused millions if not billions of lost, which potentially leading us to the next war. Heather, Nacy mentioned in his "Cyberwarfare at a Global Scale", the next major war will happen in cyberspace, the outcome will be more devastating than any other weapons. " This war has begun, cyberware hasn’t caused a major physical impact yet but it's pushing to a global scale.